(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09179951 A**

(43) Date of publication of application: **11 . 07 . 97**

(51) Int. Cl **G06K 17/00**
G06F 12/14
G06F 19/00
G09C 1/00
G09C 1/00
H04L 9/10
H04L 9/32

(21) Application number: **07349505**

(22) Date of filing: **22 . 12 . 95**

(71) Applicant: **DAINIPPON PRINTING CO LTD**

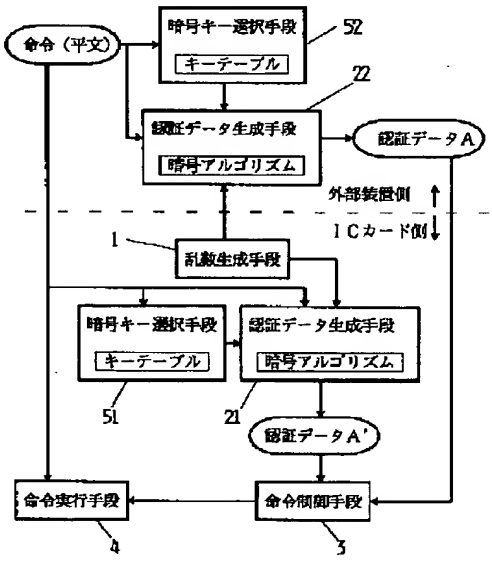
(72) Inventor: **IRISAWA KAZUYOSHI**

(54) **PORTABLE INFORMATION RECORDING MEDIUM AND ITS SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent a portable information recording medium from being illegally accessed by checking the validity of each instruction sent from an external device and then executing the instruction.

SOLUTION: The portable information recording medium is provided with a random number generating means 1, a certification data generating means 21, an instruction controlling means 3, an instruction executing means 4, a cipher key selecting means 51, and the like. The means 51 is provided with a correspondence table between instructions and cipher keys as a key table and the means 21 is provided with cipher algorithm. The portable information recording medium is an IC card having a microcomputer, an IC card and the like. The means 21 generates certification data for all or a part of an instruction sent from the external device by the use of a random number, a cipher key and the cipher algorithm and the means 3 compares the generated certification data with certification data sent from the external, device together with the instruction to certificate the validity of the instruction and permit the execution of the instruction.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－179951

(43)公開日　平成９年(1997)７月11日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｋ	17/00			Ｇ０６Ｋ	17/00	Ｅ
						Ｔ
Ｇ０６Ｆ	12/14	３２０		Ｇ０６Ｆ	12/14	３２０Ａ
						３２０Ｂ
	19/00		7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ａ

審査請求　未請求　請求項の数６　ＦＤ　（全７頁）　最終頁に続く

(21)出願番号　特願平7－349505

(22)出願日　平成７年(1995)12月22日

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号

(72)発明者　入澤　和義
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

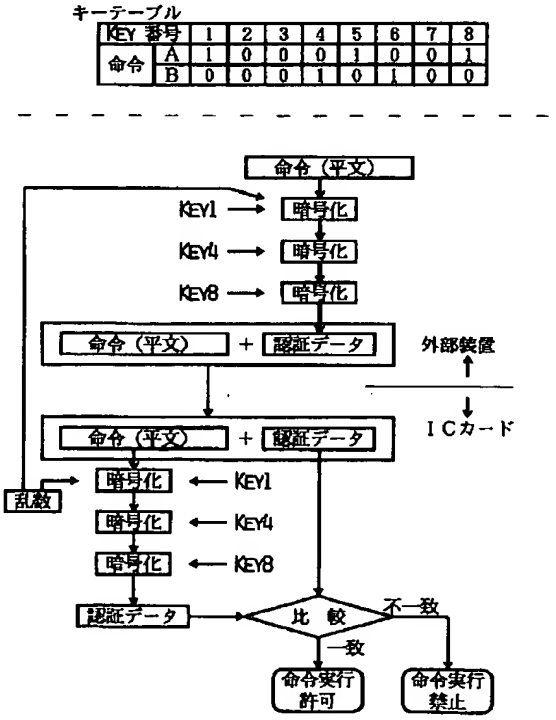
(74)代理人　弁理士　小西　淳美

(54)【発明の名称】　携帯可能情報記憶媒体及びそのシステム

(57)【要約】

【課題】　ＩＣカード等が外部から受ける命令の正当性を逐次判定して正当な場合のみ実行できる様にして、不正な外部装置からの命令を拒絶する。

【解決手段】　外部装置がＩＣカードに命令を送るときは、ＩＣカードで発生させた乱数と、外部装置自身が所有しＩＣカードと同一の暗号キー及び暗号アルゴリズムとで、その命令に対する認証データを生成し命令と共に送る。ＩＣカード側では受けた命令に対する認証データを生成し、外部からの認証データと一致していれば、その命令を認証して実行する。認証データ生成に用いる暗号キーは命令によって変わる様に複数の暗号キーの組み合わせをキーテーブル等で定義しておき選択使用する。



1

【特許請求の範囲】

【請求項１】　マイクロプロセッサとメモリとを、少なくとも有する携帯可能情報記憶媒体において、

乱数を発生する乱数発生手段と、

携帯可能情報記憶媒体自身が所有する暗号キー及び暗号アルゴリズムと、上記乱数を用いて、内部の認証データを生成する認証データ生成手段と、

外部装置からの命令と共に送られる認証データを、上記認証データ生成手段で生成した内部の認証データと比較し、前記命令の正当性を認証し命令の実行を許可する命令制御手段とを有し、

暗号キー及び暗号アルゴリズムと上記乱数を用いて外部装置から送られた命令の全部又は一部に対する内部の認証データを認証データ生成手段により生成し、命令制御手段にて該認証データを外部装置から送られた認証データと比較して、一致する場合に命令が正当であると認証して命令実行を許可する、携帯可能情報記憶媒体。

【請求項２】　認証データ生成に用いる暗号キーが、複数の暗号キー群の中から予め取り決めた任意の規則に従って命令に対応して選ばれた１又は複数の暗号キーであり、

外部装置から送られた命令を判別することで認証データ生成に用いる暗号キーを上記暗号キー群の中から選択する暗号キー選択手段をさらに備え、

認証データ生成手段は、暗号キーとして暗号キー選択手段で指定された１又は複数の暗号キーの組み合わせを用いて認証データを生成する、請求項１記載の携帯可能情報記憶媒体。

【請求項３】　複数の暗号キー群の中から命令に対応して１又は複数の暗号キーを選ぶ規則が、命令をグループ分けして同一グループ内の命令では共通の暗号キーとする、請求項２記載の携帯可能情報記憶媒体。

【請求項４】　命令制御手段は、命令実行許可条件として、内部及び外部からの認証データ同士の一致と共に、乱数発生手段で生成した乱数が外部に送られていることを条件とする、請求項１、２又は３記載の携帯可能情報記憶媒体。

【請求項５】　携帯可能情報記憶媒体がＩＣカードである、請求項１～４のいずれか１項に記載の携帯可能情報記憶媒体。

【請求項６】　請求項１～５のいずれか１項に記載の携帯可能情報記憶媒体と、外部装置とからなる携帯可能情報記憶媒体システムであって、

上記外部装置は、携帯可能情報記憶媒体が認証データ生成に用いるものと同一の暗号キーと同一の暗号アルゴリズムを所有し、

該暗号キー及び該暗号アルゴリズムと、携帯可能情報記憶媒体から取得した乱数とを用いて、携帯可能情報記憶媒体に送る命令に対する認証データを生成する認証データ生成手段を備え、

2

また、携帯可能情報記憶媒体側で認証データ生成に用いる暗号キーが、命令をグループ分けして同一グループ内の命令では共通の暗号キーとする等として、複数の暗号キー群の中から予め取り決めた任意の規則に従って命令に対応して選ばれた１又は複数の暗号キーである場合には、携帯可能情報記憶媒体に送る命令に対応して上記規則と同様な規則で上記暗号キー群の中から上記認証データ生成手段で用いる暗号キーを選択する暗号キー選択手段も備え、

携帯可能情報記憶媒体に命令を送るときは、該携帯可能情報記憶媒体側と同様にして該命令の全部又は一部に対する認証データを上記認証データ生成手段で生成して、該命令と共に認証データを送る、

携帯可能情報記憶媒体システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、集積回路としてマイクロプロセッサ及びＩＣメモリを内蔵したＩＣカードに代表される携帯可能情報記憶媒体に関する。特に、外部装置から受ける命令の正当性を判定することで、不正な外部装置を拒絶できる携帯可能情報記憶媒体に関する。

【０００２】

【従来の技術】演算処理手段としてマイクロプロセッサ、情報記憶手段としてＲＡＭ、ＲＯＭやＥＥＰＲＯＭを備えた、いわゆるＩＣカードに代表される携帯可能情報記憶媒体は、マイクロプロセッサの高度なデータ処理能力によって、内部に記憶されるデータを不正アクセスから防御できる高度なセキュリティ性を有している。例えば、外部装置から送られた暗証が内部に記憶しておいた暗証と一致する場合のみ、内部のデータへのアクセスを許可したり、或いは、携帯可能情報記憶媒体と外部装置とで共通の暗号化アルゴリズムで暗号化データを生成し、両者の暗号化データが同一の場合に内部のデータへのアクセスを許可する等の方策が取られる。そして、この様なＩＣカードに代表される携帯可能情報記憶媒体は、その優れたセキュリティ性によって、バンクカード、クレジットカード、各種の施設やクラブ等のＩＤカード、プリペイドカード等に使用されだしており、その将来性が期待されている。

【０００３】

【発明が解決しようとする課題】ところが、該携帯可能情報記憶媒体に記憶された内容を不正に書き換えたり、読み出したりする不正行為者に対する、携帯可能情報記憶媒体側の防御技術は、これで充分であるという事はありえない。例えば、ＩＣカードに予め記憶した暗証と外部装置からの暗証を比較する場合は、記憶しておいた暗証が解読されてしまえば、無防備となってしまう。また、ＩＣカード側から見て、それがセットされる端末を正当なものであると認証する端末認証は、一度ＩＣカー

ドが端末にセットされて端末を正当なものであると認証した後は、再度端末認証を行うことはなく、最初に端末認証を行った後に端末から送られる各種命令は全て正当なものとして取り扱われる。したがって、不正な端末が正当な端末を偽る余地が存在することになり、不正行為による命令をＩＣカードが受け付けてしまう恐れが発生する。

【０００４】

【課題を解決するための手段】そこで、本発明の携帯用情報記憶媒体は、上記課題を解決し目的を達成するために、マイクロプロセッサとメモリとを、少なくとも有するＩＣカード等に代表される携帯可能情報記憶媒体において、乱数を発生する乱数発生手段と、暗号キー及び暗号アルゴリズムを所有させ、前記乱数と暗号キー及び暗号アルゴリズムを用いて外部装置から送られた命令の全部又は一部に対する認証データを認証データ生成手段で生成し、これを命令制御手段で外部装置から命令と共に送られた認証データと比較することで、命令の正当性を認証し命令実行を許可する様にした。このような携帯可能情報記憶媒体に対する外部装置側には、上記と同じ暗号キー及び同じ暗号アルゴリズムを持たせて、命令を携帯可能情報記憶媒体に送る時は、その命令の全部又は一部に対する認証データを、携帯可能情報記憶媒体側で発生させた乱数を取得して、この乱数と暗号キーと暗号アルゴリズムとを用いて作成し、命令と共に携帯可能情報記憶媒体に送る。そして、携帯可能情報記憶媒体側では、外部装置から送られた命令に対して、外部装置側が行ったと同様に命令の全部又は一部に対する認証データを作成する。すなわち、外部に送った乱数と、自己の暗号キー及び暗号アルゴリズムで認証データを作成し、これが外部装置から送られた認証データと一致したときに、正当な命令であり、また、正当な外部であると認証する。そして、認証が不成立の場合は、その命令の実行を拒絶する様にした。

【発明の実施の形態】

【０００５】以下、図面を参照しながら説明する。図１は、命令によって異なる暗号キーを用いて、外部装置及び携帯可能情報記憶媒体で認証データを生成し、この認証データの認証により命令の実行可否を制御する説明図である。図２は、本発明の携帯可能情報記憶媒体側と外部装置側とからなるシステムの概略ブロック図である。

【０００６】また、本発明ではこの暗号キーを複数用いて認証データを生成する様にして、しかも、命令により用いる暗号キーの組み合わせを変える。すなわち、複数の暗号キー群の中から予め任意の規則で命令に対応して、暗号キー選択手段が選んだ１個又は複数の暗号キーを用いる。複数の暗号キー群と、命令と、用いる暗号キーの組み合わせ（１個又は複数の暗号キーからなる）の関係は、例えば、キーテーブルとして暗号キー選択手段が所有する（図１及び図２参照）。

【０００７】そして、命令に対応して暗号キーの組み合わせを変える場合、各命令毎にそれぞれ異なる組み合わせとする等と、その規則は任意である。（もちろん、携帯可能情報記憶媒体側での規則と同一の規則を外部装置側でも用いる。）該規則としては、例えば、命令をそのコマンド特権レベルに応じて複数のグループに分類して、同一のグループに属する命令に対しては、共通の暗号キーの組み合わせを使用する。或いは、命令を使用する使用者、例えば、患者のＩＤカードを兼ねた携帯可能情報記憶媒体であれば、患者、医者、薬剤師、医療事務員等といった使用者毎にグループ分けする（同一の命令が異なるグループに重複することもあり得る）等である。コマンド特権レベルでの命令のグループ分けでは、コマンド特権レベルが高いものは、用いる暗号キーの数を多くする等することもできる。また、コマンド特権レベルによってグループ分けされた命令は、その命令の使用者のグループ分けになっていることもある。また、複数の暗号キーを用いる場合、用いる暗号キーは同じであるが、命令に対して暗号アルゴリズムを操作するときに、暗号キーを用いる順番が異なる様な順番も規定した組み合わせもあり得る。なお、順番が特に無ければ、例えば、キーのＩＤ番号順とすれば良い。

【０００８】以上の様に、認証データの生成に用いる暗号キーは、携帯可能情報記憶媒体に対して共通の暗号キーを少なくとも一つ外部でも所有し、外部でもこれを用いて（又、共通の乱数及び共通の暗号アルゴリズムを用いて）認証キーを生成しないと正しい認証データは得られない。また、用いる暗号キーが一つであるということは、外部装置側で認証キー生成に用いる暗号キーのキーコードを一つ持てば最低限良いということだが、むしろ普通は、一つのキーコードからなる暗号キーをマスターキーとして用い、これと携帯可能情報記憶媒体の識別コード等とからワークキーを生成して、このワークキーを認証キー生成に用いる。従って、外部側では、携帯可能情報記憶媒体から識別コードを取得して、外部で所有している暗号キー（マスターキー）と取得した識別コードとから暗号キー（ワークキー）を生成し、これを認証キー生成に用いる。従って、上記でいう暗号キーの組み合わせは、ワークキーの組み合わせであることもあるし、マスターキーの組み合わせであることもある。

【０００９】また、外部装置側で認証データ生成に用いる乱数は、携帯可能情報記憶媒体が用いる乱数と同一のものとし、一つの乱数を両者で共用することになるが、乱数の発生は携帯可能情報記憶媒体側で行い、外部装置は携帯可能情報記憶媒体側から取得した乱数を用いる。乱数の共有化の点では、乱数発生は外部装置側で、或いは両者で共通の乱数発生アルゴリズムで別々に同一の乱数を発生させる様にするなども考えられるが、本発明の趣旨である携帯可能情報記憶媒体側から外部（の命令、ひいては外部装置）を認証する目的では、乱数発生は携

帯可能情報記憶媒体側のみが良い。外部装置側で乱数発生を行う形態では、不正に製作した外部装置がそれに都合の良い乱数を携帯可能情報記憶媒体に送ることで、携帯可能情報記憶媒体の命令認証の仕組みを解読される余地を与えることになるからである。なお、複数の暗号キーを用いる暗号化のプロセスを複数回繰り返す場合には、通常は最初の暗号化プロセスに乱数を用いるが、必ずしもこれに限定されず、例えば全部の暗号化プロセス、或いは二回目以降の暗号化プロセスに用いても良い。また、用いる乱数は、通常は連続して同一の乱数が発生しない乱数発生手段によって得る。なお、乱数発生手段は、ソフトウァア的なものであっても良く、乱数発生回路によっても良く、任意である。

【００１０】認証データ生成手段は、上記暗号キーと乱数と、所定の暗号アルゴリズムで、命令の全部又は一部に対する認証データを生成する。認証データ生成に用いる暗号アルゴリズムは任意であるが、例えば、データ暗号標準ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）が使用でき、また、その操作モードとしては例えばＣＢＣ（Ｃｈｉｐｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モードを使用すれば良い。なお、認証データ生成手段は、ソフトウァア的なものであっても良く、暗号化回路によっても良く、任意である。なお、認証データ生成の対象となる命令は、基本的には一つの命令毎である。また、外部装置から携帯可能情報記憶媒体に送る命令にはその命令のコードの他に、命令に応じて通常は引数等のコード列が連なるが、本発明では命令の種類によって用いる暗号キーを変えるので、少なくとも命令の種類が分かれば良く、例えば命令コード部分だけでも良い。或いは引数部分も含めた全命令文等とすれば、認証データの対象となるコード列のビット長が大きくなり、安全性はより高くなる。或いは、命令のコードの一部でも、命令をグループ分けする形態では、その一部のコードが共通なものを共通なグループとしても良い。なお、命令に対する引数は、例えば、ＲＥＡＤ＿ＢＩＮＡＲＹ命令ではファイルＩＤと読出し相対アドレスと長さ等が引数となり、ＷＲＩＴＥ＿ＢＩＮＡＲＹ命令ではファイルＩＤと書き込み相対アドレスと書き込みデータ等が引数となり、ＵＰＤＡＴＥ＿ＢＩＮＡＲＹ命令では、ファイルＩＤと書換え相対アドレスと書換えデータ等が引数となる。

【００１１】以上の様にして、外部装置から送られた平文の命令に対して携帯可能情報記憶媒体は認証データを内部で作成し、これを命令制御手段が前記平文の命令に対応して送られた認証データと比較し、一致する場合はその命令が正当であると認証し、その命令の実行許可を出す。一致しない場合は命令実行を許可しない。そして、命令制御手段の命令許可がある場合のみ、命令実行手段は外部から送られた命令を実行する。

【００１２】なお、本発明の携帯可能情報記憶媒体が記憶するデータの格納形式等は任意であり、特に制限はないが、例えば、書き換え可能に格納されるデータは、ＥＰＲＯＭ等のＩＣメモリに図４の様な階層構造で格納する。同図においては、メモリ領域のユーザーデータ領域全域を管理するＭＦ（マスタファイル）に対して１又は複数のＤＦ（データファィル）が割り当てられる。携帯可能情報記憶媒体が複数の用途に使用される場合には、各用途毎にこのＤＦが割り当てられる。また、ＤＦに対してもＤＦが割り当てられることがある。これは、或る用途の中でもデータを細分して格納する等の為である。そして、各用途で利用する取引データ等はＷＦ（ワークファイル）に格納される。また、ＷＦのアクセス権獲得に必要なファイルアクセス制御に関する暗号キー等はＫＦ（キーファイル）として格納される。また、ＭＦ自身も携帯可能情報記憶媒体として必要なデータをＷＦに、暗号キー等をＫＦとして所有している。以上の様なファイルの階層構造、或いは、或るデータ領域、すなわちＷＦに対するアクセス権の為のＫＦを格納する形式は、従来のＩＣカード等と同様であ。そして、本発明で使用する認証データ生成の為の暗号キーも、上記暗号キー同様に上記ＫＦとして格納しておけば良い。なお、ＫＦは特別な特権が無いとアクセスすることが出来ない様になっている。また、キーテーブルも各用途毎のＤＦに対して、或いは各用途共通でＭＦに対して等と、格納しておけば良い。

【００１３】

【実施例】以下、本発明を一実施例により説明する。図２は本発明の携帯用情報記憶媒体及び外部装置とからなるシステムの一実施例のブロック図である。携帯可能情報記憶媒体は、乱数生成手段１、認証データ生成手段２１、命令制御手段３、命令実行手段４、暗号キー選択手段５１等を備えている。暗号キー選択手段５１は命令と暗号キーとの対応表をキーテーブルとして備え、認証データ生成手段２１は暗号アルゴリズムを備えている。また、この携帯可能情報記憶媒体は、マイクロコンピュータとＩＣメモリ等を有するＩＣカードであり、この他の構成は、従来公知のＩＣカードと同様である。例えば接触型のＩＣカードの場合はマイクロコンピュータＭＰＵ（ＭｉｃｒｏＰｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）を中心に、ＭＰＵの動作プログラム等を格納したＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、作業用メモリのＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、各種利用データ、暗号キー、暗号アルゴリズムの格納メモリのＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　ａｎｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、また、必要に応じて乱数発生させる乱数回路、暗号アルゴリズの演算処理を行う暗号化回路、ＭＰＵと外部装置との電気的接続を行う入出力コネクタ等から構成される（入出力コネクタは非接触型の場合は不要である）。乱数回路、暗号化回路

等は、これらをソフトウェア的に行うのであれば不要である。なお、メモリは通常はＭＰＵ経由でないとアクセスできない構造となっている。

【００１４】一方、端末等の外部装置側でも、携帯可能情報記憶媒体と同様にして認証データを生成できる様に、認証データ生成手段２２、暗号キー選択手段５２等を備えている。また、その他の構成はシステムの用途により従来公知の機能を備えている。そして、外部装置側では携帯可能情報記憶媒体に送る平文の命令に対して、認証データＡを生成し、平文の命令に対応して携帯可能情報記憶媒体に送る。

【００１５】そして、携帯可能情報記憶媒体側では、送られた命令に対して認証データＡ′を生成し、これを前記認証データＡと比較して認証を行い、命令の実行或いは拒絶をすることとなる。

【００１６】図１は、複数の異なる暗号キーの組み合わせが命令によって使用される様子を示した説明図である。キーテーブルには、複数の暗号キーがキー番号１～８として登録されており、これに命令Ａ及びＢ（ここでは説明の都合二種類とした。Ａ及びＢは一つの命令として考えても良いし、グループの区分と考えても良い）で、異なる暗号キーを選択して用いる事が示されている。具体的には、命令Ａには、キー番号１、５及び８の暗号キーを、命令ＢにはキーＮｏ４及び６を用いることを示している。このキーテーブルは外部装置側と携帯可能情報記憶媒体側の両方で同一のものをそれぞれ所有する。図１の例では、命令として命令Ａを携帯可能情報記憶媒体に送るので、外部装置は、キーテーブルを参照して、暗号キーにＫＥＹ１とＫＥＹ４とＫＥＹ８とをその順番で暗号化操作に順次用いて平文の命令を暗号化して認証データを得る。なお、同図の場合では、携帯可能情報記憶媒体から所得した乱数は、ＫＥＹ１を用いる最初の暗号化プロセスにのみ使用する。

【００１７】次に、図３のフロー図にて、外部装置と携帯可能情報記憶媒体との処理の流れを説明する。外部装置は、先ずＧＥＴ＿ＣＨＡＬＬＥＮＧＥ命令を携帯可能情報記憶媒体に送り、携帯可能情報記憶媒体から乱数を取得する（ステップＳ１）。なお、この乱数取得命令は、認証データが不要であり認証なしで携帯可能情報記憶媒体は命令実行する。次に、外部装置は携帯可能情報記憶媒体に送る平文の（引数が含まれ得る）命令（文）のデータの後ろに、８の倍数のなるように０（ゼロ）をパディングした後、認証データを命令の一部に対するものとして作成すべく、命令の先頭８バイトと前記乱数とを排他的論理和で演算する。次いで、携帯可能情報記憶＊媒体側と同じ規則によりその命令で用いる暗号キーを選択し（ステップＳ２）、選択された暗号キーを用いて暗号関数ＤＥＳのＣＢＣモードにより、得られた暗号化データを再度暗号化する操作を暗号キーの数だけ次々に繰り返して、最終的に得られた８バイトの暗号化データを認証データＡとして生成する（ステップＳ３）。そして、この認証データＡを前記命令とともに携帯可能情報記憶媒体に送る（ステップＳ４）。一方、携帯可能情報記憶媒体側では、受信した命令から用いる暗号キーを選び（ステップＳ５）、前記乱数とこの暗号キーと暗号アルゴリズムにより、受信した命令に対して、外部装置と同様な操作で認証データＡ′を生成する（ステップＳ６）。そして、外部からの認証データＡと内部で生成した認証データＡ′とを比較して、一致しておればその命令は正当であると認証して命令の実行を許可し（ステップＳ７）、携帯可能情報記憶媒体は受信した命令を実行する（ステップＳ８）。不一致であれば命令は認証されず命令の実行は拒絶される（ステップＳ９）。

【００１８】以上の様にして、本発明では、携帯可能情報記憶媒体は外部から受ける命令について、その正当性を認証しながら実行することになる。

【００１９】

【発明の効果】本発明によれば、外部装置からの命令に対して、その命令毎にその正当性を確認した上で命令実行が成されるので、不正にアクセスされる事の無い高いセキュリティ性が得られる。また、接続の途中で命令を捏造された場合でも、その検知が可能になる。

【図面の簡単な説明】

【図１】本発明の携帯可能情報記憶媒体及びそのシステムによる命令の認証動作を説明する説明図。

【図２】本発明の携帯可能情報記憶媒体及びそのシステムの一実施例の概略ブロック図。

【図３】本発明の携帯可能情報記憶媒体及びそのシステムの処理の流れを説明するフロー図。

【図４】本発明の携帯可能情報記憶媒体におけるファイル構造の一例。

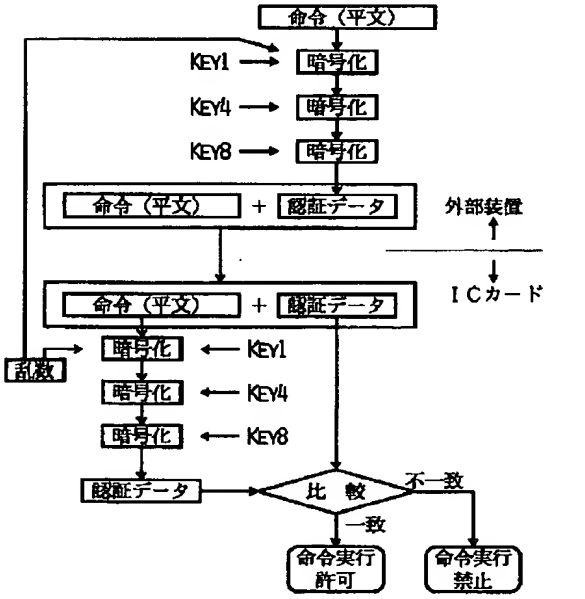
【符号の説明】

１　乱数生成手段
２１　認証データ生成手段（携帯可能情報記憶媒体側）
２２　認証データ生成手段（外部装置側）
３　命令制御手段
４　命令実行手段
５１　暗号キー選択手段（携帯可能情報記憶媒体側）
５２　暗号キー選択手段（外部装置側）
Ｓｎ　ステップ番号

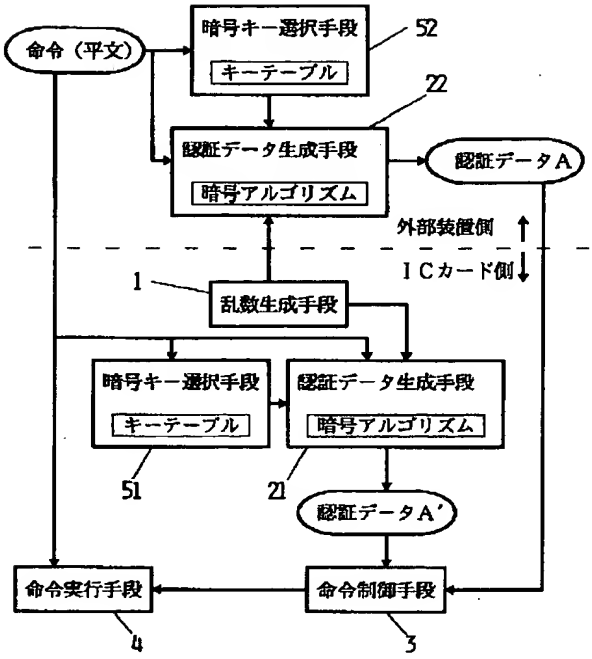
【図１】

キーテーブル

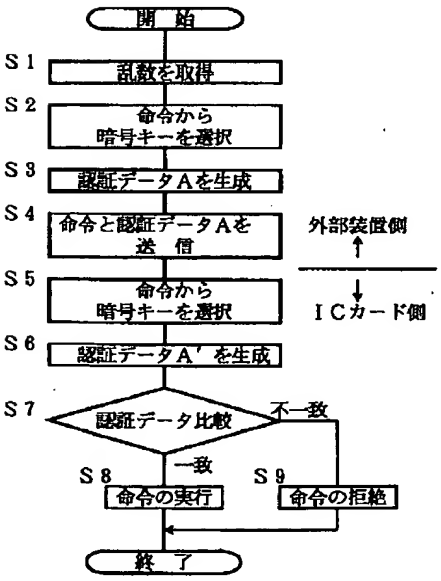
KEY 番号		1	2	3	4	5	6	7	8
命令	A	1	0	0	0	1	0	0	1
	B	0	0	0	1	0	1	0	0



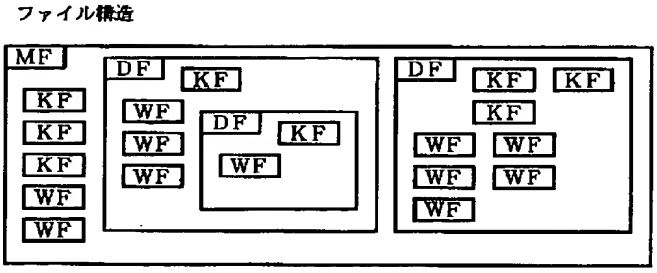
【図２】



【図３】



【図４】



フロントページの続き

(51) Int. Cl.[6]		識別記号	庁内整理番号	F I		技術表示箇所
Ｇ０９Ｃ	1/00	６４０	7259－５Ｊ	Ｇ０９Ｃ	1/00	６６０Ａ
		６６０		Ｇ０６Ｆ	15/30	３４０
Ｈ０４Ｌ	9/10					３５０
	9/32			Ｈ０４Ｌ	9/00	６２１Ａ
						６７３Ｂ
						６７３Ｃ